العنوان:	الإجراءات الاحترازية الدولية في مواجهة خطر الإرهاب الإلكتروني : التجربة الفرنسية نموذجاً
المصدر:	المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية- ICACC - كلية علوم الحاسب والمعلومات - جامعة الإمام محمد بن سعود الإسلامية - السعودية
المؤلف الرئيسي:	أبو عمار، ميلود عبدالرحمن بنعتيك
محكمة:	نعم
التاريخ الميلادي:	2015
مكان انعقاد المؤتمر:	المملكة العربية السعودية. الرياض
رقم المؤتمر:	1
الهيئة المسؤولة:	جامعة الإمام محمد بن سعود الإسلامية. كلية علوم الحاسب والمعلومات
الشهر:	نوفمبر
الصفحات:	138 - 151
رقم MD:	690622
نوع المحتوى:	بحوث المؤتمرات
قواعد المعلومات:	HumanIndex
مواضيع:	الإرهاب الإلكتروني
رابط:	http://search.mandumah.com/Record/690622

الإجراءات الاحترازية الدولية في مواجهة خطر الإرهاب الإليكتروني التجربة الفرنسية نموذجا

ميلود عبد الرحمن بنعتيك أبو عمار (•)
جامعة مولديا بوليس
الدار البيضاء، المغرب
Miloud.2006@yahoo.fr. M.benatik@mundiapolis.ma

الملخص – من أهم وأخطر وسائل الإرهاب في العصر الحديث الإرهاب الإلكتروني المتمثل في العدوان أو التخويف أو التهديد مادياً أو معنوياً باستخدام الوسائل الإلكترونية الصادر من الدول أو الجماعات أو الأفراد على الإنسان في دينه ونفسه أو عرضه، أو عقله، أو ماله، بغير حق بشتى صنوفه وصور الإفساد في الأرض.

وأن استخدام الإنترنيت أصبح منتشراً انتشاراً واسعاً وهذا مما سهل نقل المعلومات فيما بين الأفراد والجماعات، وما بين الدول والمنظمات، ولكن نجد أنه في الآونة الأخيرة إساءة استخدام هذا الاختراع التقني حيث أصبح يمثل إرهاباً إلكترونياً عالمياً يهدد العالم بأسره، ويمكن خطر توظيف الأنترنيت باعتباره لا لجنسية له ولا حدود جغرافية تحده، حيث يقوم الإرهابي بأعماله التخريبية عن بعد وهو غائب – جسميا – عن مسرح الجريمة بل ومن خلف عالم افتراضي غير مادي.

لقد أضحي الإرهاب الإلكتروني هاجساً يخيف العالم الذي أصبح عرضة لهجمات الإرهابيين عبر الإنترنت، الذين يمارسون نشاطهم التخريبي في أي مكان في العالم.

وتعتبر وسائل التواصل والاتصال الإليكترونية التي توفرها شبكة الانترنيت من أهم الوسائل في التواصل بين الإرهابيين وتبادل المعلومات فيما بينهم، لذلك يقوم المخربون المعتدون باستغلال هذه التقنيات التواصلية في نشر أفكارهم والترويج لها والسعي لتكثير الأتباع والمتعاطفين معهم عن طريق الاستقطاب والاسترداج ثم التجليد.

في هذا العرض الوصفي بعد عرضنا لماهية هذا النوع من الإرهاب وأهدافه وأسبابه وآثاره ...، عرجنا على طرح الجهود الدولية لمواجهة هذا السرطان "الافتراضي" حيث كانت شاملة لما هو تقني وتشريعي وفني .... ثم أخيرا حاولنا الكشف عن أهم معالم التجربة الفرنسية في مكافحتها للإرهاب الإليكتروني حيث وظفت فيها الوسائل المؤسساتية والقانونية والتكنولوجية وأشركت جميع المعنيين بمعالجة هذه الظاهرة حتى تضمن لأمنها القومي فضاء رقمياً آمنا باعتباره مطلبا وطليا وفق رؤية دولية.

الكلمات المفتاحية – الإرهاب الإلكتروني: الإنترنيت؛ التقنيات التواصلية؛ فرنسا؛ الجهود الدولية؛ الأمن القومي؛ الفضاء الرقمي التوعية الاستباقية.

1. المقدمة

أضحت ظاهرة الإرهاب تؤرق القاصي والداني، الفقرة والغني، الأفراد والمجموعات، الشعوب والحكومات، عربيا، وإقليميا، وإسلاميا ودوليا، كما تعددت أشكالها والتي تمس السلم والأمن على المستوي العالمي، وبناء على النتائج الكارثية الناجمة عن هذه الظاهرة على أمن وسلامة الأفراد والجماعات، فإن لهذا آثارا وخيمة على الثروات المادية وغير المادية للدول بالإضافة إلى المس المباشر بسيادة هذه الدول كل على حدة بل تتعدي ذلك إلى التجمعات الإقليمية والدولية.

وإن هذا الخطر استدعي ويستدعي، من الجهات الرسمية، تكاثف الجهود والتنسيق لوضع الخطط الإستراتيجية والبرامج التفصيلية والمرحلية لمواجهة ظاهرة الإرهاب والحد من آثارها وتحجيمها إلى حين القضاء عليها وعلى مسبباتها، إلى جانب ذلك فإن المؤسسات البحثية للدراسات الأكاديمية والعلمية أعطت الظاهرة نصيبها من الاهتمام والبحث والدراسة، ناهيك عن منظمات المجتمع المدني التي تسعي ببرامجها وفعالياتها إلى تعميم الوعي بين فئات المجتمع تربية وتأطيرا ومرافقة لتحصين المجتمع من هذه الآفة، ونظرا للتطور المتسارع لوسائل الإعلام والاتصال والتواصل فإن هذه الأخيرة أعطت بدورها لهذا الأمر العناية اللازمة له من خلال البرامج الإذاعية والتغطيات الصحفية والتقارير التلفزية لتنوير الرأي العام المحلي والعالمي بحقيقة وأبعاد هذا السرطان المدمر وفضح وسائله وأنواعه وأشكاله وأساليبه وآلياته، كما وأن المنظمات الدولية ذات الاهتمام بمكافحة الإرهاب أعطت لهذه الظاهرة أولية قصوى مع تعيين موارد

(•) بالإضافة إلى وظيفته الرسمية أمينا لمكتبة أكاديمية للتعليم العالي بجامعة مونديابوليس فهو استشاري جمعوي، وسيط ثقافي ومدير موقع الرقاص للفعاليات العلمية والأكاديمية

هامة لمساعدة الدولي في مجهوداتها الرامية إلى التحصين من الإرهاب ومكافحته. ولعل أهم المؤشرات التي يتطلب من خلالها الرفع من مستوي المعالجة والتنسيق بين كل المتدخلين والمعنيين بمحاربة الإرهاب هو اعتماد هذا الأخير في إحدى أحدث وأخطر صوره؛ على شبكة الإنترنت التي تعتبر من أهم اختراعات العصر الحديث؛ ألا وهو الإرهاب الإلكتروني أو الإرهاب الرقمي أو الإرهاب عن طريق الإنترنت أو الإرهاب المعلوماتي.

ولقد كانت فرنسا من بين الدول الأوائل التي سعت إلى تحصين مواطنيها وأراضيها وأمنها القومي من أخطاره. وفي هذا الإطار فقد سنت عدة تشريعات واعتمدت العديد من التدابير والإجراءات الاحترازية كان اخرها التعديل التشريعي الذي يعزز من أمنها والحد من تجنيد مواطنيها للإلتحاق بصفوف من تعتبرهم الدولة الفرنسية بالجماعات التكفيرية وما يسمي بـ "داعش"[1] العراق وسوريا.

الفقرة الأولى ماهية الإرهاب الإلكتروني وتعريفه

تعددت التعاريف المعطاة لمصطلح إرهاب، إلا أن الدارسين والخبراء والمهتمين من كل المشارب والتوجهات، بل وحتى المؤسسات الرسمية ذات الاهتمام، أجمعوا واتحدوا على أن غايته لا يمكن أن تنفصل عن كونه مسببا لإذاية الآخرين إما إذاية مادية أو معنوية.

ومن جانب آخر فقد تعددت أشكال الإرهاب من إرهاب عسكري إلى آخر جرثومي إلى إرهاب الاقتصادي إلى آخر إليكتروني، أو رقمي أو معلوماتي.

وإذ نقتصر في عرضنا هذا على ما هو إليكتروني فإنه وقياسا على تعريف للإرهاب أصدره مجمع الفقه الإسلامي الدولي ضمن قرارات دورته الرابعة عشرة المعقودة في الدوحة في شهر ذي القعدة من عام 1423هـ [2] يمكن تعريف الإرهاب الإلكتروني بأنه العدوان أو التخويف أو التهديد ماديا أو معنوياً باستخدام الوسائل الإلكترونية الصادر من الدول أو الجماعات أو الأفراد على الإنسان دينه، أو نفسه، أو عرضه، أو عقله، أو ماله، بغير حق بشتى صنوفه وصور الإفساد في الأرض.

ويعتبر هذا التعريف من التعاريف الاصطلاحية المتميزة من حيث الفهم المستوعب للإرهاب على مستوي الشمولية وضبط سلوك الإرهاب وفعله [3].

الفقرة الثانية: الإرهاب الإلكتروني وأثره

لعل في التطوير الهائل الذي عرفته الإنسانية على مستوي وسائل الاتصال والمعلومات ما جعل الاعتماد على التقنية الحديثة يشمل جميع مناحي الحياة الشخصية والمهنية، الفردية والمؤسساتية، إلا أنه وفي مقابل الاستعمال السليم والآمن لهذه التقنية فإن هناك من له مقصد وغاية سيئة في توظيف هذا الاختراع البشري، وقد عرف العالم ويعرف حاليا من اكتوي من الاستعمال الضار لهذا الاختراع والمتمثل في الإرهاب الإلكتروني.

---

[1] فصيل من أكبر الفصائل المقاتلة حاليا في العراق وسوريا وتعني كلمة داعش المختصرة، الدولة الإسلامية في العراق والشام، هذا وقد غير هذا الفصيل اسمه فيما بعد إلى "الدولة السامية"

[2] مجمع الفقه الإسلامي/ قرارات وتوصيات الدورة الرابعة عشرة للمجلس/ قطر/ 1423هـ.

[3] للاستئناس ولمزيد من الإيضاح نورد هناك بعض التعاريف المتداولة عن الإرهاب الإلكتروني باعتباره (حسب مجلة المعلوماتية وهي مجلة دورية حائزة على ترخيص من رئاسة مجلس الوزراء، وتصدر بشكل شهري عن الجمعية العلمية السورية للمعلوماتية) ينطلق من تعريف الإرهاب، حيث يعرفه مجمع البحوث الإسلامية بالأزهر بأنه: (ترويع الأمنين، وتدمير مصالحهم ومقومات حياتهم، والاعتداء على أموالهم وأعراضهم وحرياتهم، وكرامتهم الإنسانية، بغياً وإفساداً في الأرض)، أما بالنسبة للاتفاقية العربية لمكافحة الإرهاب فإنها عرفت الإرهاب بأنه، (كل فعل من أفعال العنف أو التهديد به أيا كانت دوافعه أو أغراضه يقع تنفيذاً لمشروع إجرامي فردي أو جماعي ويهدف إلى إلقاء الرعب بين الناس أو ترويعهم بإيذائهم أو تعريض حياتهم أو حرياتهم أو أمنهم للخطر أو إلحاق الضرر بالبيئة أو بأحد المرافق أو الأملاك العامة أو الخاصة أو احتلالها أو الاستيلاء عليها أو تعريض الموارد الوطنية للخطر). أما بالنسبة لمصطلح "الإرهاب الإلكتروني" الذي ظهر وشاع استخدامه عقب الظفرة الكبيرة التي حققتها تكنولوجيا المعلومات واستخدامات الحواسب الآلية والإنترنت تحديداً في إدارة معظم الأنشطة الحياتية، وهو الأمر الذي دعا 30 دولة إلى التوقيع على "الاتفاقية الدولية الأولى لمكافحة الإجرام عبر الإنترنت"، في بودابست، عام 2001، والذي يعد وبحق من أخطر أنواع الجرائم التي ترتكب عبر شبكة الإنترنت فإنه يمكن تعريفه "بأنه" هجمات غير مشروعة، أو تهديدات بهجمات ضد الحاسبات أو الشبكات أو المعلومات المخزنة إلكترونياً، توجه من أجل الانتقام أو ابتزاز أو إجبار أو التأثير في الحكومات أو الشعوب أو المجتمع الدولي بأسره لتحقيق أهداف سياسية ودينية أو اجتماعية معينة، وبالتالي فلكي ينعت شخصاً ما بأنه إرهابياً على الإنترنت، وليس فقط مخترقاً، فلا بد وأن تؤدي الهجمات التي يشنها إلى عنف ضد الأشخاص أو الممتلكات، أو على الأقل تحدث أذي كافياً من أجل نشر الخوف والرعب"، فالإرهاب الإلكتروني إذن وكما أوردته هيئة تقنية المعلومات العمانية على موقعها الرقمي يعتمد على استخدام الإمكانيات العلمية والتقنية، واستغلال وسائل الاتصال والشبكات المعلوماتية، من أجل تخويف وترويع الآخرين، وإلحاق الضرر بهم، أو تهديدهم.

أن الأثر المباشر للإرهاب الإلكتروني يظهر جليا في خطورته البالغة بل والأدهى والأمر هو يسر استعمال هذه التقنية كسلاح مدمر مع بالغ أثره وتعدد أضراره.

إن التطور المتسارع والهائل الذي يعرفه قطاع الاتصالات والمعلومات يسري على منحيين متعارضين، أولها التوظيف السليم للتقنية في خدمة مصالح الإنسانية ومن ذلك على سبيل المثال لا الحصر التقنيات الأمنية والبحث المتتالي على آليات وسبل توفير أنظمة للتصفح الأمن على شبكة الإنترنيت، وثانيهما الاستعمال الضار للقرصنة الإلكترونية وتوظيف التقنية لخرق المواقع على شبكة الإنترنيت وكسر حواجزها الأمنة عبر البحث المضني في الكشف على الثغرات الأمنية.

إن الإرهاب الإلكتروني أضحي إشكالا يؤرق جميع الدول المتقدمة والفقيرة على حد سواء والتي أصبحت عرضة للمجرمين الذين يرهبون الأفراد والجماعات عبر شبكة الإنترنت حيث يمارسون أفعالهم التخريبية عن بعد، وتبقي الجهود الدولية على مستوي اتخاذ التدابير والاحترازات لمكافحة الواجة الإلكترونية للإرهاب غير ذات جدوى لحصر أخطار هذا السرطان الرقميي.

الفصل الأول: واجهات الإرهاب الإلكتروني

الفقرة الأولى: واجهة تصميم المواقع الإلكترونية وإنشاؤها

من أيسر الأساليب الحديثة في التواصل والاتصال ونقل المعلومات وترويجها هو توظيف الإعلام الرقمي من خلال إنشاء وتصميم مواقع إليكترونية على الشبكة العنكبوتية، وهذا ما يسر على الإرهابيين إنشاد مواقع وصفحات على الشبكة للترويج لأفكارهم واستقطاب ذوي العقول الضعيفة والضمائر المهزوزة لحمل مبادئهم وتوجهاتهم التخريبية، بل إن العديد من المواقع المتصلة بهؤلاء المجرمين تقوم بإتاحة أساليب ومناهج وآليات ومساطر إجرائية لكيفية القيام بالجرائم التخريبية الإرهابية، ومن ذلك كيفية اختراق المواقع الحكومية والرسمية، وأساليب صنع العبوات الناسفة، وكيفية تدمير المواقع والبريد الإلكتروني عبر الفيروسات الفتاكة.

إن المجتمع الرقمي سهل بشكل كبير تواجد الإرهابيين وتواصلهم فيما بينهم عبر عدة وسائل إليكترونية توفرها الإنترنيت مثل غرف الدردشة الآنية، والمواقع الإلكترونية على الويب، ومنتديات الحوار، ومواقع الهاتف الرقمي المجاني سكايب مثلا وغير ذلك...

أضحت الإنترنيت الملاذ الأمن الإرهابيين لما توفره لهم من وسائل رقمية اتاحتها ثورة الاتصالات والمعلومات وتطور المعلوميات بشكل متسارع، فأصبح للجماعات الإجرامية والإرهابية العديد من العناوين والمواقع والمنتديات على شبكة الويب العالمية، فأصبحت بذلك تلك المواقع من الواجهات الرئيسية المستعملة في الإرهاب الإلكتروني.

ولا شك أن ترويع الناس من خلال إنشاء المواقع للعدوان وتضليل الآخرين ونشر الأفكار الهدامة محرم ولا يجوز من الناحية الشرعية ووفق مبادئ الإسلام السمحة. وفي هذا الصدد فقد صدرت فتوى شرعية [1] تقول: شبكة الإنترنت من وسائل الاتصالات الحديثة السريعة في إيصال المعلومات الواسعة من حيث الانتشار وسهولة الوصول إليها وهي إن استغلت في الخير والدعوة إلى الله ونشر دين الله في أصقاع الأرض من قبل الأفراد والمؤسسات الإسلامية المختلفة، فلا شك أنها من الجهاد في سبيل الله بالبيان واللسان ويجب على المسلمين استغلالها وتسخيرها لهذا الغرض الخير، أما المواقع الفاسدة المخلة والمضرة بعقائد المسلمين من خلال التلبيس والتشكيك والمضرة بأخلاقهم كذلك من خلال ما يعرض فيها من الدعوة إلى الفساد وتيسير طرقه وتعليم الناشئة لهذه الأمور، وتربيتهم عليها من خلال ما يعرض فيها ... فلا ريب أن هذا من أعظم المنكرات التي يجب التصدي لها وإنكارا وفق قواعد إنكار المنكر التي جاء بها النص من الكتاب والسنة، وبينها وفصلها علماء الأمة، والله تعالي يقول: " **وَلْتَكُن مِّنكُمْ أُمَّةٌ يَدْعُونَ إِلَى الْخَيْرِ وَيَأْمُرُونَ بِالْمَعْرُوفِ وَيَنْهَوْنَ عَنِ الْمُنكَرِ وَأُوْلَئِكَ هُمُ الْمُفْلِحُونَ (104)**" [2]. وفي حديث لمسلم وقال صلي الله عليه وسلم: من رأي منكم منكراً فليغيره بيده، فإن لم يستطيع فبلسانه، فإن لم يستطع فبقلبه، وذلك أضعف الإيمان) [3].

الفقرة الثانية واجهة اختراق وقرصنة المواقع الإلكترونية

إن الولوج غير المشروع على نقطة ارتباط أساسية أو فرعية مرتبطة بالويب من خلال نظام آلي أو مجموعة نظم مترابطة شبكيا بغرض تدمير نقطة الاتصال أو تخريب النظام هو ما يقصد بالاختراق والقرصنة.

---

(1) سماحة مفتي عام المملكة الشيخ عبد العزيز بن عبد الله آل الشيخ

(2) سورة آل عمران الآية 104.

(3) أخرجه الإمام مسلم في كتاب الإيمان 691.

ونظرا للمستحدثات الإلكترونية المتسارعة ومعرفة المخربين بنقاط ضعف الأنظمة وثغرات التطبيقات جعلت من الصعوبة بما كان الحيلولة دون خرق وقرصنة المواقع، وذلك ناجم عن التحيين المستمر والتحديث المتتالي في منتديات الإرهابيين وغرف الدردشة للتقنيات والمعلومات ذات الأغراض الإرهابية فبات من أولى أولويات عملهم ومبادئهم السعي إلى اختراق وتدمير المواقع وقرصنتها.

إن القرصان الرقمي والإرهابي الإلكتروني المسمي بالهاكر له من الخبرة والتقنية ما يؤهله إلى الوصول إلى "المعلومات السرية والشخصية واختراق الخصوصية وسرية المعلومات بسهولة، وذلك راجع إلى أن التطور المذهل في عالم الحاسب الآلي يصحبه تقدم أعظم في الجريمة المعلوماتية وسبل ارتكابها، ولاسيما وأن مرتكبيها ليسوا مستخدمين عاديين، بل قد يكونون خبراء في مجال الحاسب الآلي (1).

وتقول المزروعي عن الكيفية التي تتم بها عملية الولوج غير المشروع للموقع الرقمي بأنها أي عملية الاختراق الإلكتروني تتم عن طريق تسريب البيانات الرئيسة والرموز الخاصة ببرامج شبكة الإنترنت، وهي عملية تتم من أي مكان في العالم دون الحاجة إلى وجود شخص المخترق في الدولة التي اخترقت فيها المواقع فالبعد الجغرافي لا أهمية له في الحد من الاختراقات الإلكترونية ولا تزال نسبة كبيرة من الاختراقات لم تكتشف بعد بسبب التعقيد الذي يتصف به نظام تشغيل الحاسب الآلي (2).

وعلى اعتبار أن معرفة البيانات التفصيلية لمتصفح الإنترنيت أضحت من أيسر المعلومات الخصوصية التي يمكن لأي كان له أدنى مستوى من المعرفة بالويب وتقنياتها أن يلج إليها فإن الهاكر لا يجد أدنى صعوبة في كشف طبيعة مستخدمي الإنترنيت وهوياتهم.

إن من بين الطرق التي توظف لتدمير المواقع هو إمطار الموقع المستهدف بالآلاف من الرسائل الإلكترونية من جهاز الكومبيوتر الخاص بالإرهابي قصد التأثير على الطاقة الاستيعابية للموقع، وبهذه الطريقة تتم قرصنة معظم المواقع الرسمية وعناوين البريد الخاص بالأفراد أو المؤسسات على حد سواء.

ويمكن تعداد معالم ضعف الأنظمة الأمنية الإلكترونية إلى العديد من العوامل نذكر منها ما يلي:

1. عدم اكتراث مستخدم الإنترنيت بالجانب الأمني لمعطياته الشخصية ومدي أهميتها لدي القراصنة والإرهابيين لتوظيفها في الأعمال الإرهابية والتخريبية.
2. استهانة مستخدمي الإنترنيت بخطورة مغادرة شبكة الإنترنيت دون إغلاق تام ونهائي للبريد الإلكتروني أو الصفحات الإليكترونية الخاصة أو الحسابات الخاصة في غرف الدردشة والمنتديات وصفحات مواقع التواصل الاجتماعي.
3. تيسير الولوج إلى الحسابات الشخصية من خلال اعتماد كلمات سرية بسيطة وسهلة جداً، مما يسهل على القرصان المخرب الوصول إلى تخمين كلمة السر واختراق البريد أو الموقع.
4. الاكتفاء باعتماد برامج حماية مجانية متاحة على الويب لا تتوفر فيها شروط الحماية الرصينة والدائمة للموقع من الاختراق أو القرصنة.
5. الغفلة عن التحديث الدائم والمستمر لبرامج الحماية والتي تقوم تلقائيا وآلياً بالتنبيه عند وجود حالة اختراق للموقع أو محاولة قرصنته وتخريبه، بل في كثير من الأحيان يتم أساسا إغفال التحديث المستمر لنظام التشغيل.
6. الحرص على إنشاء الموقع على يد مؤسسات متخصصة لكن ليس في مقدورها توفير الدعم التقني المستمر، أو أنها تقوم باستغلال برامج وأنظمة مجانية أو رخيصة غير موثوقة من الناحية الأمنية كما أنه لا يتم تحيينها بشكل دوري.
7. عدم القيام بمراجعة التحديثات الخاصة بجديد الفيروسات ومدي تطورها وخطورتها.

الفقرة الثالثة نظام المراسلات الإليكترونية والمحادثة الآنية

يرتكز عمل نظام المراسلات الإلكترونية على خدمة البريد الإلكتروني التي توفر إمكانية تبادل الرسائل ذات الطبيعة الرقمية والمعلومات الإلكترونية مع الغير عبر شبكة الإنترنيت، ويعتبر نظام المراسلات الإليكترونية من أهم الخدمات التي توفرها الشبكة العنكبوتية لمستخدميها الافتراضيين، حيث يمكن إرسال أو التواصل بالرسالة الرقمية في وقت قياسي في أي مكان على وجه البسيطة.

وانطلاقا من هذا المعطي فقد أصبح البريد الإلكتروني من أخطر الوسائل الموظفة في الإرهاب الإلكتروني، حيث توفر هذه الوسيلة الرقمية سرعة التواصل بين الإرهابيين والتنسيق التام فيما بينهم عبر تبادل المعلومات والخطط والبرامج، وحسب آخر التقارير

---

(1) سهير حجازي/ التهديدات الإجرامية للتجارة الإلكترونية/ شرطة دبي

(2) موزة المزروعي/ الإختراقات الإلكترونية خطر كيف نواجهه/ مجلة آفاق الاقتصادية، دولة الإمارات العربية المتحدة، العدد التاسع، سبتمبر 2000م، ص 54.

والدراسات الأمنية فإن جل العمليات الإرهابية والعمليات التخريبية والجرائم الإلكترونية الأخيرة كانت الوسيلة المعتمدة فيها هي البريد الإلكتروني.

ومن الناحية "الدعوية" والترويج لنشر الأفكار والمبادئ التي يؤمن بها ويتبناها ذووا التوجهات الإرهابية الاستقطاب وتجنيد المتعاطفين فإنهم يقومون باستمالة أصحاب العقول الضعيفة والتأثير فيهم من خلال الرسائل الإلكترونية. كما أن للإرهابيين طرقهم الخاصة وأساليبهم في التجسس على المعطيات الشخصية لمستخدمي البريد الإلكتروني من خلال اختراق الحسابات الخاصة بالأفراد أو المجموعات وهتك أسرارهم وكشف معلوماتهم وبياناتهم الشخصية عبر تصفح مراسلاتهم واستغلالها للقيام بعملياتهم الإرهابية والتخريبية.

ومن بين الأمثلة الحية على خرق وقرصنة البريد الإلكتروني للأشخاص معايشتي للعديد من الحالات التي تم فيها اختراق لحسابات بعض معارفي، ومن بينهم مدير مركز استشفائي بمدينة فاس المغربية، حيث قام قرصان من إحدى الدول الإفريقية بقرصنة حسابه وتوظيف هذا الأخير في انتحال شخصية طبية ومحاولة السطو على أموال معارف وأصدقاء هذا المدير.

أما المحادثة الآنية عبر المنتديات المفتوحة منها والمغلقة، وعبر غرف الدردشة المسماة بصالونات "الشات"، ومن خلال المحادثة عبر مواقع التواصل الاجتماعي، فهي بدورها لا تقل أهمية عن البريد الإلكتروني من خطورتها وتوظيفها في الدعاية للأفكار والعمليات الإرهابية، بحيث توفر هاته التقنيات إمكانية اجتماع افتراضي على مستوي عالمي لحاملي الفكر الإرهابي ولمروجيه بأعداد لا يمكن حصرها أو ضبطها. كما أنها توفر تبادل المعلومات والخطط التخريبية بشكل آني وعلى مستوي عالي من السرعة والانتشار. ومن جانب آخر فإن المحادثة الآنية تساعد المخربين على الترويج لأفكارهم الهدامة والإجرامية واستقطاب واستدراج المستهدفين السذج من مستخدمي العالم الافتراضي وتقنيات التواصل الاجتماعي.

الفصل الثاني: الإجراءات الإحترازية لمواجهة الإرهاب الإلكتروني

الفقرة الأولى: ضبط وتصفية خدمات تصفح الإنترنت

نظرا للهجوم المتسارع لثورة المعلومات والاتصالات والتقنيات المعلوماتية، بات لزاما على الأفراد والمؤسسات حماية أنفسهم وأوطانهم من آثار هذا التطور التكنولوجي الهائل والتدفق السريع لهذه التقنية وسرعة انتشارها بين البلدان والمجتمعات، لأنها إلى جانب محاسنها فهي تحمل في طياتها العديد من المخاطر المادية وغير المادية التي تتطلب من مكونات المجتمع الوطني والدولي مواجهاتها بحسم حتى لا تحصل تلك المخاطر بأشكالها وأنواعها المختلفة.

والجدير بالذكر أن من أهم التدابير الاحترازية والوقائية على مستوي الشبكة المعلوماتية هو ضبط وتصفية خدمات تصفح الإنترنيت عبر حجب المواقع التي تدعم الإرهاب وتروج لأفكاره وتنادي بالعدوان والاعتداء على الغير. ويعتبر هذا التدبير من الإجراءات الناجعة التي تحصن المواطنين والدول، والمؤسسات والهيئات من تداعيات هذه المواقع وما تحويه من سراطانات هدامة للعقول والمقدرات والممتلكات وغير ذلك. ونذكر على سبيل المثال بعض الدول والحكومات التي سارعت إلى ضبط وحصر الولوج إلى خدمة تصفح الإنترنيت عبر الحجب والرقابة والمصادرة الدول التالية: كوريا الشمالية، وجمهورية مصر العربية، والمملكة العربية السعودية، والمغرب، وتركيا ثم فرنسا ... وغيرها كثير من الدول التي سعت إلى حجب المواقع الفتاكة وتصفية الإنترنيت من الصفحات الهدامة عبر اعتماد الأجهزة والآليات التكنولوجية التي تقوم بتنقية المواقع المشبوهة وحجبها بل ومنع ظهورها على شبكات الإنترنيت الوطنية.

الفقرة الثانية: التشريعات والتقنيات الإلكترونية

تعد التشريعات والقوانين الإلكترونية من أهم إفرازات عصر المعلومات. فقد أثارت البيئة الرقمية أو الإلكترونية جملة من التحديات والمشكلات القانونية التي تطلبت تنظيماً قانونياً في جانب منها لعدم تعرض القوانين القائمة في الدول العربية والغربية لتنظيمها أو تتطلب إعادة تقييم للقواعد القائمة للتتوائم مع الطبيعة الخاصة لتطبيقات العصر الرقمي أو الإلكتروني، ومن أبرز التحديات القانونية في هذا الحقل تحديات الجرائم الإلكترونية والعمليات الإرهابية من خلال الفضاء الرقمي.

وأيضاً تحديات التنظيم القانوني للبنية التحتية، وتتعلق بالتنظيم القانوني لخدمات الاتصال وتزيد خدمة الإنترنت وجهات الإشراف على الأعمال الإلكترونية.

ويندرج في نفس الإطار تحديات حماية الأوطان والمواطنين وتنفيذ القانون، ومسائل أمن المعلومات وتوفير الحصانة المعلوماتية القانونية.

ويري محمد القاسم أن تقنية المعلومات باتت تجذب إليها العديد من المتعطشين لقضاء مآربهم الحياتية وتوفير الاحتياجات اليومية للأفراد والمؤسسات مما أدي إلى تجلي "الحاجة الملحة إلى إيجاد أنظمة لضبط التعاملات الإلكترونية بشتى صورها، فعلي الرغم من محدودية ما أنجز في هذا السياق فإن الجهات التي تضطلع بهذه المهام تعاني من البطء الشديد في إنجاز هذه الأنظمة لكثرة الجهات الممثلة في لجان الصياغة وتعدد الجهات المرجعية التي تقوم بمراجعة الأنظمة واعتمادها، لذا فلا بد من إعداد الأنظمة اللازمة لتحقيق الاستفادة القصوى من تقنية المعلومات، وحماية المتعاملين من المخاطر التي تنطوي عليها تلك التقنيات، ولقد أظهرت استبانة أجريت للتعرف على مدي الحاجة إلى وجود تنظيمات ولوائح تحكم قضايا تقنية المعلومات أن 70% يرون الحاجة إلى ذلك" [1].

وإذا كان الكمبيوتر والإنترنت وغيرهما له فوائد جمة بالنسبة لبشرية عموما إلا أن المخاطر المترتبة على سوء استخدام هذه التقنيات كبيرة وكثيرة، وكما نعلم أن الشريعة الإسلامية والقوانين المرعية والتشريعات الدولية من جهة لا تحارب العلم، بل تدعو إليه وتحبذه، لكننا رأينا أن هذه التقنيات العلمية التي لا ترفضها التشريعات والقوانين ترتب على استخدامها جرائم تلحق الأذى بالغير وتضر بمصالحه، لذا كان لا بد من وقفه قانونية وتشريعية مع هذه الوسائل العلمية الحديثة والمعاملات المترتبة على توظيف هذه التقنيات الحديثة. وفي هذا المجال يؤكد صاحب دراسة الوضع الراهن في مجال أحكام في المعلوماتية على أنه "وبالرغم من إدراك أهمية وجود وتطبيق أحكام وأنظمة لضبط التعاملات الإلكترونية فإن الجهود المبذولة لدراسة وتنظيم ومتابعة الالتزام بتلك الأحكام لا يزال في مراحله الأولية، وما تم في هذا الشأن لا يتجاوز مجموعة من القرارات المنفصلة واللوائح الجزئية التي لا تستوعب القضايا المستجدة في أعمال تقنية المعلومات، كما لا توجد بصورة منظمة ومعلنة أقسام أمنية، ومحاكم مختصة، ومنتجات إعلامية لشرائح المجتمع المختلفة [2].

الفقرة الثالثة: الوسائل التقنية للوقاية من العمليات الإرهابية الإلكترونية

تواجه الجريمة الإرهابية ذات الطبيعة الإلكترونية في ظل العولمة التكنولوجية، تحديات كبيرة في مواجهتها ومحاربتها، على اعتبار الوسائل التقنية التي توظفها من جهة، وتنوع مظاهرها وتعدد واجهاتها من جهة أخرى، فتلك الجرائم كثيرة ومتنوعة وسريعة، وتشمل كافة نواحي الحياة الاجتماعية والاقتصادية والثقافية وأيضاً الأمنية، مما يجعل هذه الجرائم تعتبر مسا خطيراً لأمن الدولة والمواطنين.

وقد أجمع كل المعنيين بأمن الشبكة على أنه لا يوجد حل جذري ينصح به للوقاية من جرائم الحاسب الآلي بأشكالها المختلفة، "إلا أنه يجب وضع إستراتيجية أمنية شاملة لنظم المعلومات تحدد عناصرها ومسئوليات الدخول إلى نظم المعلومات، كما يجب وضع خطة طوارئ دقيقة اختيارها ومراجعتها بصفة دورية [3]".

أما عن تحديات مواجهة الجريمة الإرهابية التقنية في ظل نظام العولمة، فقد قدم "مارتن ناجيمان M. Nabgman" تقريراً حول "أوربا ومجتمع المعلومات العالمي" أو ما يسمي بمجتمع الإعلام الكوكبي، وقد نشر التقرير في يوليو 1994م، وقد تضمن التقرير خطة عمل ضمن أربعة محاور رئيسية، وقد كانت أهم نقطة في التقرير هي "ضرورة سرية البيانات وحماية حقوق الملكية الفكرية" [4].

وقد ناقش وزراء خارجية دول الاتحاد الأوروبي مشروع يسمح بحماية أسس البيانات، هذا بالإضافة إلى قرارات مؤتمر قمة الدول الصناعية السبعة في فبراير من عام 1995م.

ولما كان لجرائم الإنترنت هذه الخطورة على أمن الفرد والمجتمع، وبخاصة ما يتعلق بحرية البيانات والمعلومات الخاصة بكل فرد أو مؤسسة، وخاصة أن تلك الجرائم تمثل اعتداءاً على النفس والعرض والمال وغيرها. وكذلك ما تمثله هذه الجرائم من تهديد للأمن القومي للمجتمعات على مستوي العالم، ما يتبع ذلك من آثار اجتماعية وثقافية واقتصادية سلبية، "لذلك يجب وضع البرامج والأساليب والطرق الحديثة الفعالة للتعامل مع هذا الواقع الجديد الذي فرض نفسه على الأفراد والمجتمعات على مستوي العالم كله [5].

إنه لمن الخطأ إذا النظر إلى الإرهاب كظاهرة جامدة فهو نشاط إنساني لا يتوقف عن تطوير آلياته، وصوره، وأدواته، والإرهابيون اليوم باتوا أكثر تنظيماً، وذكاء، في ظل معطيات التقنية التي سهلت التكوين، والتدريب، والاتصال، والتواصل ومن بين

---

(1) محمد القاسم (ضمن فريق عمل)/ دراسة الوضع الراهن في مجال أحكام في المعلوماتية/ مشروع الخطة الوطنية لتقنية المعلومات

(2) مرجع سابق

(3) صالح المسند، 2000م، 190

(4) محمد الرومي، 2003، 112 – 113.

(5) صالح المسند، 2000م، 194.

وسائل مكافحة الإرهاب الإلكتروني الكثيرة، يجب تقسيم عناصر مكافحة الإرهاب الإنترنت تقنيا وفنيا، تبعا لمكوناتها الفنية، وعناصرها المختلفة على النحو التالي: أمن المواقع، وأمن الأجهزة، وأمن البرامج.

وبناء عليه يقوم معظم المهتمين والمعنيين بحماية وأمن الشبكة حول العالم الآن بتوفير الخدمات علي الإنترنت التي تتطلب تبادل البيانات الخاصة بحماية هاته الأخيرة على الإنترنت من أي استغلال من لدن الهاكرز والإرهابيين المختفين وراء أسماء أو منظمات أو شخصيات وهمية وافتراضية، ومثال على ذلك ينصح المكتب الاتحادي لأمان تكنولوجيا المعلومات في ألمانيا بضرورة الاعتماد على اتصال مشفر بالإنترنت عند التعامل بواسطة بطاقات الائتمان في المعاملات المالية الإلكترونية على سبيل المثال حتى لا يتم قرصنة الموارد المالية للمستخدم لأغراض إرهابية وتخريبية.

كما يتعين على المستخدم عدم إدخال أية بيانات إلا إذا كان موقع الويب محمياً بواسطة تقنية التشفير SSL، التي يمكن التعرف عليها من خلال ظهور الاختصار "https" في شريط العنوان عند زيارة مثل هذه المواقع.

علاوة على أن العديد من برامج تصفح الإنترنت تقوم بتمييز الاتصالات المشفرة بواسطة ظهور رمز القفل أيضاً في شريط العنوان. وتظهر الصفحات والمواقع الإلكترونية الجيدة والمأمونة بعض الأرقام فقط، وعند استعمال أرقام البطاقات الائتمانية تظهر هذه الأخيرة على هيئة نجوم صغيرة.

وبالإضافة إلى الاتصال الآمن والمشفر بشبكة الإنترنت، ينبغي أيضاً أن تشتمل التجهيزات الأساسية لأي حاسوب على برامج مكافحة الفيروسات والشفرات الضارة، بالإضافة إلى وجود جدار الحماية المعروف باسم الجدار الناري.

ويؤكد خبراء المكتب المذكور على أهمية تثبيت آخر التحديثات الأمنية التي يتم طرحها لنظام التشغيل والبرامج المستخدمة بصورة منتظمة، حتى لا يتمكن القراصنة ودعاة الإرهاب من استغلال الثغرات الأمنية في متصفح الإنترنت أو نظام التشغيل لاختراق حواسب المستخدم والحصول على المعلومات الهامة بواسطة برامج "حصان طروادة" (تروجان).

ومع ذلك لا تجدي كل إجراءات التأمين نفعاً إذا كان المستخدم يكشف عن بياناته الشخصية طواعية إذا ما تعرض لهجمات القراصنة بواسطة رسائل التصيد، حيث يتظاهر الإرهابيون في مثل هذه الرسائل أنهم ممثلون عن الهيئات الرسمية التي يتعامل معها المستخدم أو المواقع الإلكترونية الموثوقة.

لهذا يجب على المستخدم أن يعلم يقينا بأن المنظمات والهيئات والمؤسسات الرسمية الإلكترونية الحقيقة لا تستعلم أبداً عن أرقام بطاقات الشخصية والبيانات الخصوصية وأكواد "PIN" أو "TAN" عن طريق رسائل البريد الإلكتروني، ولذلك يتعين على مستخدم النت حذف مثل هذه الرسائل على الفور إذا ما ظهرت في صندوق البريد الوارد.

الفصل الثالث: جهود فرنسا لمكافحة الإرهاب الإلكتروني

فرنسا والإرهاب: نظرة تاريخية [1]:

عرفت فرنسا في الفترة ما بين 1972 و1987 الإرهاب عندما كانت المنظمات الشيوعية المقاتلة تستخدم أوروبا مسرحا للجريمة. ويشار إلى أنه في أوائل الثمانينيات كانت فرنسا مسرحا لاعتداءات اعتبرتها إرهابية حصلت بين المهاجرين من جنسيات معادية لبعضها البعض. وتحت تأثير موقف فرنسا المؤازر للولايات المتحدة في الصراع الفلسطيني الإسرائيلي عرفت فرنسا بعض العمليات التي كيفتها على أنها إرهابية، بدأت بحادث قطار باريس – تولوز في 22 مارس سنة 1982 مستهدفا مصالحها السياسية والاقتصادية وشعبها.

وعرفت فرنسا في الفترة من 1985 و1986 نوعا من الإرهاب تحت تأثير بواعث سياسية ودينية. ويشار إلى أنه منذ سنة 1993 بسبب سياسة فرنسا في دعم سياسة الحكومة الجزائرية تجاه الإسلاميين جعلها هدفا لهجمات تنظيم الجهاد، وأنه في الفترة من 1996 إلى 1999 تضاعفت الخلايا الإرهابية في أوروبا وأتخذت أسلوب تنظيم القاعدة، وما بين ديسمبر سنة 2000 وأبريل سنة 2001 كشفت الأجهزة الإيطالية والألمانية والفرنسية خلية إرهابية تخطط لمهاجمة كاتدرائية استراسبورج وفي 12 سبتمبر سنة 2001

(1) نقلا وبتصرف شديد عن الدكتور أحمد فتحي ي سرور/ حكم القانون في مواجهة الإرهاب (القاهرة: سنة 2007) راجع مجلة جوست عدالة

2 Nothalie cettina; the French approach: Vigaur and vigilonce, (in Marianne Van levrven, confronting terrorism, ap. Cit., p. 71 etc.

بدأ مكتب الإدعاء العام في باريس تحقيقات أولية للبحث في فرنسا عن إمكان وجود شركاء للأحداث الإرهابية التي وقعت في الولايات المتحدة 2.

وقد بدأت فرنسا في تأسيس سياستها الجنائية على أربعة مبادئ هي: التخصص، والمركزية، والتنسيق المنظم، والاتصال وتبادل المعلومات بين مختلف الأجهزة لبحث العلاقة بين أفراد الخلايا الإرهابية. وقد اقتضت هذه المبادئ إنشاء إدارات متخصصة ومركزية داخل الشرطة لمواجهة الإرهاب، بجانبها قضاء متخصص في هذا النوع الخطير من الجرائم.

وقد التجأت فرنسا ابتداء في محاربة الإرهاب إلى قانون العقوبات وقانون الإجراءات الجنائية، مع الأخذ بنظام قانون يخالف القواعد العامة واعتبار العمل الإرهابي وصفا له ذاتيته القانونية، ولم يترتب على مخالفة القواعد العامة في نصوص قانوني العقوبات والإجراءات الجنائية أي نقد جوهري من جانب المجلس الدستوري الفرنسي الذي أكد في 3 سبتمبر سنة 1986 أن نصوص محاربة الإرهاب تجد تبريرها في الطابع الخاص للإرهاب (1).

وفي 23 يناير سنة 2006 صدر في فرنسا قانون مكافحة الإرهاب الفرنسي متمثلاً في إجراء تعديلات على القانون رقم 73 الصادر في 21 يناير سنة 1995 بشأن التوجيه ووضع البرامج في مجال الأمن، وعلى قانون الإجراءات الجنائية وقانون البريد والاتصالات، وقانون الأمن الداخلي، وقانون العقوبات، والقانون المدني، والقانون المتعلق بحرية الاتصالات، وقانون النقد والتمويل، والقانون المنظم للأنشطة الخاصة في مجال المراقبة والحراسة ونقل الأموال، وقانون الطيران المدني، وقانون التأمين، والقانون الخاص بحرية الصحافة، والقانون الخاص بتنظيم وتعزيز الأنشطة البدنية والرياضية.

وبمقتضى القانون الصادر سنة 2006 طرأ نوعان من التعديلات المباشرة على قانون العقوبات الفرنسي، الأول يتضمن إنشاء جرائم عدم القدرة على تبرير وجود موارد تتعلق بسير الحياة أو عدم القدرة علي تبرير مصدر المال، وتسهيل تبرير الموارد المشبوهة لدي الأشخاص (المواد: 321 – 6، 321 – 6 – 1، 321 – 10 – 1 عقوبات فرنسي)، والثاني بشأن الجماعات الإرهابية وذلك بتشديد العقاب على مديريها، والتوسع في تجريم هذه الجماعات بالنظر إلى الجرائم التي تحضر لها (المواد: 421 – 21 و421 – 5/ 1 و421 – 6).

واستحدث قانون الإجراءات الجنائية المادة 706 – 24 إجراءات التي تسمح لرجال الضبط القضائي بعدم إظهار شخصياتهم إلا من خلال أرقامهم المسجلة إداريا، مع معاقبة من يظهر شخصياتهم بطريقة غير مشروعة (المادة 706 إجراءات).

كما تضمن تعديلات على قانون الإجراءات الجنائية نصت على مركزية محاكم تطبيق العقوبات بباريس (التي تشرف على تنفيذها) بشأن المحكوم عليهم في جرائم إرهابية، وإنشاء محاكم جنايات متخصصة للأحداث الإرهابية (المادة 706 – 25)، والتدخل الاستثنائي لقاضي الحريات لإطالة القبض الذي يمارسه مأمور الضبط garde a vue في حالة توافر خطر جوي ينذر بوقوع عمل إرهابي.

كما استحدث هذا القانون نظاما لتحسين تعويض ضحايا الأعمال الإرهابية (2).

وكانت فرنسا من الدول التي اهتمت بتطوير قوانينها الجنائية للتوافق مع المستجدات الإجرامية حيث أصدرت في عام (1988م) القانون رقم (19 – 88) الذي أضاف إلى قانون العقوبات الجنائي جرائم الحاسب الآلي والعقوبات المقررة لها.

الفقرة الأولى: معالم الإستراتيجية الفرنسية في مواجهة الإرهاب الإلكتروني

التهديد الإرهابي الإليكتروني لم يكن ينظر إلى قوته وخطورته، حيث عرف تغييرا عميقا في طبيعته. وسريا علي نهج معظم شركائها، كيفت فرنسا مجهوداتها في هذا السياق الجديد. وقد عزز قانون 23 كانون الثاني 2006 حول مكافحة الإرهاب الاستجابة المتطلبات الوقاية وفق المتغيرات السريعة في وسائل النقل وتقنيات الاتصالات. وقد أسفرت هذه الجهود عن وضع إستراتيجية طويلة الأجل، تم عرضها ضمن الكتاب الأبيض لمواجهة الإرهاب والذي يعتبر جزء من الجهود الرامية إلى مكافحة الإرهاب وفق أنجع السبل. وهذا الكتاب هو ثمرة تفكير بين المهنيين ورجال المخابرات والقضاة والمسئولين الحكوميين والصحفيين والأكاديميين. وإنه بالإضافة إلى التكيف الاحترازي جنبا إلى جنب مع ثمرات التعاون الدولي، فإن الفرنسيين يعتبرون أن التعبئة على أوسع نطاق هي الكفيلة بمواجهة

---

(1) 3cc, Dec du 3 sept 1986 no 86 – 213.

(2) La loi no 2006 – 64 du 23 janvier 2006 relative a la lutte contre le terrorism, rev. sc crim 2006, no 2, p 366.

تحدي الإرهاب. وهذا ينطوي على معلومات واضحة عن واقع التهديد ووسائل تنفيذها لمواجهة الموقف. هذه هي الرسالة الرئيسية لهذه الوثيقة الهامة [1].

وجاء الكتاب الأبيض حول الأمن الداخلي ضد الإرهاب في فرنسا ثمرة التنسيق المحكم بين مكونات وهياكل الدولة الحيوية. وهذه الوثيقة جاءت واضحة المعالم ومحدد الأهداف ومهمة على مستوي الرؤية الإستراتيجية التي رسمت لها. وهذا يدل على أن فرنسا، رغم أنها لا تتبني الرؤية الأمريكية في الحرب ضد الإرهاب، إلا أنها من خلال كتابها الأبيض تعكس تماما مدي جهوزيتها أمام الخطر الحاذق بالدولة حيث سارعت إلى مواجهة الموقف عبر عدة مسارات.

إن الكتاب يعتبر التهديد الإرهابي بأنه عالمي وإستراتيجي وبناء عليه رسم الخطوط العريضة لمواجهة حصرية حول تهديد بعينة حدده في التهديد "الجهادي"، وهذه النقطة تستحق مزيدا من النقاش لعدم الإشارة إلى بعض التهديدات الأخرى الناجمة عن الجماعات غير الإسلامية والتي لا يتم تناولها في الوثيقة.

الأهم من ذلك، يقول الكتاب الأبيض أن كلا من فرنسا وأوروبا تتفقان شكل واضح على أنهما هدفان مباشران للتهديدات الإرهابية بكل تلاوينها خصوصا الإليكترونية منها على اعتبار توفر عدة عوامل تزيد من درجات التهديدات التي تواجهها.

الجزء الثاني من الوثيقة هو وصف للإجراءات والاحترازات الفرنسية المضادة للإرهاب عبر شبكة الإنترنيت كما يسلط الضوء على عدد من الأوراش المؤسساتية المفتوحة كإشكالية التواصل في الأزمات والكوارث التي تتطلب مزيدا من النظر المعمق والفاحص والسريع.

أما في جزئه الثالث فيسعي الكتاب إلى إشراك المواطنين أنفسهم في توفير أمنهم وسلامتهم، والتعامل مع الظاهرة وفق رؤية ثلاثية الاتجاهات: أولا: "المعركة اليومية" (مسئولية المواطنين، والفاعلين الاجتماعيين وقوات الأمن). ثانياً: "المعركة التكنولوجية" بحيث يهدف من هذه الاتجاه إلى "استباق التهديد" ثم ثالثاً "معركة الأفكار" التي تسعي إلى خلق التماسك الاجتماعي لعزل الإرهابيين فكريا وثقافيا [2]...

الفقرة الثانية: المجلس الوطني للرقمنة: التأسيس والمهام

تعريف المجلس الوطني للرقمنة Le Conseil National du Numérique

المجلس الوطني للرقمنة (CNN أو CNNum) هو هيئة فرنسية استشارية مستقلة عن أجهزة الدولة الفرنسية، وقد أنشئ بتاريخ 29 أبريل 2011 بموجب المرسوم رقم 2011 – 4761 وأعيد تنظيمه بموجب المرسوم رقم 2012 – 1400 من 13 ديسمبر 2012 الذي صودق عليه بتاريخ 15 ديسمبر 2012، من أجل توسيع مهام المجلس إلى معالجة الإشكالات والأسئلة التي تنتج عن التطور الرقمي.

مهام المجلس الوطني للرقمنة

باعتباره هيئة مستقلة سياسيا يعتبر المجلس الوطني للرقمنة بفرنسا محاورا ومستشارا لدي الحكومة الفرنسية، ولدي البرلمانيين، ولدي الفاعليين المهنيين ثم لدي السلطات الإدارية المستقلة. كما أن له جميع الصلاحيات للمبادرة باقتراحات بخصوص مواضيع معينة دون سابق طلب من أي جهاز حكومي، إلى جانب ذلك فإنه يعتبر قوة اقتراحية من أجل تطوير الإنترنيت في فرنسا، فضلا عن ذلك فإن من مهام المجلس إبداء وجهة نظره فيما يهم مجال تخصصه.

وفي خطاب إعلان تأسيس المجلس ذكر نيكولا ساركوزي يومها بأن هذه الهيئة تأسست على مبدأ الاستقلالية باعتبارها حرة في توصياتها وقراراتها [3].

---

(1) La France face au terrorisme: Livre blanc du Gouvernement sur la sécurité intérieure face au terrorisme (texte imprimé) / France. Premier Ministre; France, Secrétaire. – Paris: La Documentation française, 2006. – 1 vol. (141 p.); 24 cm.
ISBN: 978 – 2 – 11 – 006101 – 0, Langues: Français (fre)

(2) JH (2006). ((La France face au terrorisme. Livre blanc du gouvernement sur la sécurité intérieure face au terrorisme.)), La Documentation Française. Paris, 2006, 141 p, http://www.dsi-presse.com//p=1494 (Consulté le 16/ 09/ 2014).

(3) Sarkozy installe le Conseil national du numérique, Acteurs publics. Com, Antoine Laurent, 27 avril 2011.

وتأسيسا على مبدأ الخصوصية والسرية فإن أعضاء المجلس لهم كامل الصلاحية في تكوين فرق عمل تنصب أيضا على معالجة وبحث ودراسة القضايا ذات الطابع الاقتصادي كالضريبة على العائدات الإعلانية والإشهارية، بالإضافة إلى القضايا ذات الاهتمام العام كالعناية بالطفولة والصحة ورعاية ذوي الاحتياجات الخاصة [1]. ومن بين المهام التي من صلاحية المجلس النظر فيها محاربة التنزيل غير المشروع للملفات والبرمجيات [2].

الفقرة الثالثة: المجلس في مواجهة آخر تهديدات الإرهاب الإلكتروني.

كجزء من مهمته الاستشارية باعتباره مؤسسة ذات الاستقلالية تامة، ثم بتاريخ 25/ 06/ 2014 توجيه الدعوة إلى المجلس الوطني للرقمنة من قبل وزير الداخلية للانعقاد قصد التعليق على التشريعات الجديدة الموجهة لتعزيز الأحكام المتعلقة بمكافحة الإرهاب خصوصا أن فرنسا تعاني بشكل مباشر من تجنيد مواطنيها في الجماعات المقاتلة في العراق وسوريا. ويتم استقطاب هؤلاء المواطنين عن طريق النوافذ المتنوعة المتوفرة على فضاء الإنترنيت.

وعلى إثر هذا الاجتماع أصدر هذا الأخير توصيته التي تمت الموافقة عليها بإجماع تام من طرف جميع أعضاء المجلس في دورته هاته. وقد انصبت التوصية على توضيح رأي المجلس بخصوص الفصل 9 من مشروع القانون حول تشديد الاحترازات والتشريعات ذات الارتباط بمستجدات مكافحة الإرهاب [3].

وقد سعت هذه التشريعات والقوانين إلى الالتفاف على السلطة القضائية وعدم اعتباره من خلال الاكتفاء بالترخيص الإداري لحجب المواقع الإليكترونية التي تحتوي على عبارات وصور وكل ما من شأنه أن يشكل تحريضا على الإرهاب أو تساعد في الدفاع عن الإرهاب والترويج له.

كما أن ذات القانون موضوع تقويم المجلس يفيد بتوسيع إجراءات ونطاق آليات المراقبة المفروضة على شركات الخدمات التقنية.

هذا وعرف هذا القانون تقييما وتقويما من لدن المجلس الوطني للرقمنة حيث أصدر توصيته (بمثابة رأي نقدي) بما يلي:

يعتبر المجلس أن قرار حجب أو إغلاق المواقع التي تستقطب وتستدرج مستخدمي الإنترنيت للتجنيد في صفوف الجماعات الإرهابية غير فعال من الناحية الفنية والتقنية.

ويعتبر أن نفس الإجراء لا يتماشي والأساليب المستحدثة والمعتمدة من لدن الإرهابيين في مناهجهم الخاصة بالاستقطاب والاستدراج ثم التجنيد.

أما الانتقاد الثالث فيصب حول إغفال القانون الجديد لدور القضاء والتقليل من شأنه، حيث سيمس هذا الإجراء من الحق في الضمانات الكافية لحظ الحريات.

من شأن آليات بديلة مؤمنة وآمنة أن تكون فعالة عوضا عن الحجاب الإداري على مستوي مزودي خدمات الإنترنيت.

في المقابل أدلي المجلس بعدة إقتراحات مساعدة للفريق الحكومي والبرلمانيين في عملهم ضد الإرهاب الإليكتروني بحيث يعتبرها جد ناجعة وتحترم في نفس السياق الضمانات المكفولة للحقوق والحريات وهي على الشكل التالي:

في أفق خلق التوازن بين فعالية الإجراءات الاحترازية وعدم المس بالحريات يجب تطوير إجراءات مزدوجة تتطلب فعلاً متناسقاً بين السلطات القضائية والسلطات الإدارية مستوحي من الإجراء القائم بخصوص الألعاب الإليكترونية على النت.

تنمية وتطوير البحث العلمي من أجل فهم أعمق لأسس ومعالم التطرف في الفضاء الإليكتروني كما في المواقع الملموس.

إدماج وإشراك كل الفاعلين على مستوي شبكة الإنترنيت وأسس البيانات من أجل تطوير المعرفة وتنمية الإجراءات وأساليب التشوير بالموازاة مع مرافقة وتوجيه وإرشاد مستخدمي الإنترنيت

تعزيز التنسيق على المستوي الدولي بواسطة آليات فعالة توازي الإجراء الدولي PHAROS

([1]) Le Conseil national du numérique, I' élite des professionnels de l`économie numérique, Actualités du droit, Marlène Trézéguet, 4 mai 2011.

([2]) Nicolas Sarkozy officialise le Conseil national du numérique, Le Nouvel Observateur, 27 mars 2011.

([3]) المادة 9 تسعي لوضع حد لبث رسائل التحريض على "الجهاد" وتجنيد مقاتلين محتملين عبر الإنترنت، فالمشروع ينص على عقوبة سبع سنوات سجنا لكل من بث رسائل جهادية. كذلك يمكن أن يتم حجب بعض المواقع وعددها 160 التي أعلن عنها في 2013: والمشروع يقدم مهلة 24 ساعة إلى المحرر والمضيف، للسماح لهم بإزالة المحتوى بأنفسهم قبل حجب الموقع.

هذا وقد تأسس موقف المجلس على هذا النحو اعتبارا لخالصات جلساته المتعددة مع خبراء الأرهاب من علماء الاجتماع، رجال الأعلام، ممثلي جمعيات الضحايا دون إغفال القضاة والمحامون المتخصصون، وممثلي المجتمع المدني وأعضاء عن المؤسسات الاستخباراتية ثم مهنيي وخبراء المجال الرقمي.

الفقرة الرابعة: الفضاء الرقمي الآمن [1] مطلب وطني وفق رؤية دولية:

تجري معالجة مسألة أمن الفضاء الإلكتروني وفق التوجهات الفرنسية على مستويين وهما:

- مكافحة استعمال الفضاء الإلكتروني للأغراض الإجرامية؛
- الحماية من الانتهاكات التي تمس بحسن سير أنظمة المعلومات والاتصالات.

تشجع اتفاقية مجلس أوروبا الخاصة بأمن الفضاء الإلكتروني التي وقعت في بودابست في عام 2001، التعاون في المجال القانوني بين الدول لمكافحة ما يلي:

- الجرائم التي تستهدف السرية؛
- سلامة البيانات والنظم المعلوماتية وتوفرها للاستعمال
- التزييف والتزوير المعلوماتيان؛
- انتهاكات حقوق الملكية الفكرية.

كما تجرم الاتفاقية نشر الأعمال الإباحية التي تستغل الأطفال عبر الوسائط الإلكترونية. يمثل ترويج هذه الاتفاقية أولوية من أولويات فرنسا التي تشارك مشاركة فاعلة في إعداد التوجيه الجديد للاتحاد الأوروبي بشأن الهجمات التي تستهدف نظم المعلومات.

وتتطلب حماية نظم المعلومات هذه تحسين ضبط الفضاء الإلكتروني. لذا تؤيد فرنسا تحديد معايير للسلوك في الفضاء الإلكتروني وبخاصة للدول، وتؤيد أي تدبير كفيل بتحسين حماية البنى التحتية الحساسة للمعلومات على المستويين الوطني والدولي.

يعتبر الإنترنت محركا للنمو الاقتصادي وواسطة للممارسة الحرية والديمقراطية. بيد أنه فضاء يمكن فيه أيضاً للقراصنة وشتى أنواع المجرمين بل والدول ارتكاب أفعال محمية وغير خاضعة للعقاب.

وقد تطورت أنواع الأخطار التي ينطوي عليها الإنترنت بسرعة شديدة ومنها التجسس الإلكتروني وتشويش الشبكات والخدمات والتدمير المادي بواسطة الهجمات الافتراضية. وقد أصبحت البلدان وبناها التحتية الحيوية ومصارفها وحتى اقتصادها معرضة للشلل بفعل الهجمات المعلوماتية.

وكان رد فعل الدول في مواجهة هذا الفضاء الافتراضي المتناقض تعزيز اليقظة وحماية نظم المعلومات الحكومية والبنى التحتية الحيوية، وحتى التزود بالوسائل المضادة، بل وأيضاً دراسة السبل القانونية الكفيلة بالحد من المخاطر الملازمة للإنترنت.

وعلى الصعيد الدولي أصبح الفضاء الإلكتروني، كما كان ممكنا في السابق أن تصبح الفضاءات الجديدة – مثل البحر والفضاء الخارجي للغلاف الجوي – رهانا دبلوماسيا يتمثل في السؤال التالي: كيف يمكن تحقيق استقرار الإنترنت وأمنه؟

واعتمدت البلدان في المنظمات الدولية مواقف معاكسة بشأن تعزيز أمن الفضاء الإلكتروني، فبعض البلدان تعتقد أنه يجدر إعداد صك قانوني دولي ملزم يؤطر التدابير التي تتخذها الدول، بينما تعتبر بلدان أخرى على خلاف ذلك، أن الدول ليست الجهات الفاعلة المعنية الوحيدة وأنه يجب أيضا العمل بشراكة مع المنشآت والمجتمع المدني من أجل إعداد حلول ترمي إلى تعزيز أمن الفضاء الإلكتروني.

وتخشى هذه البلدان من أن تؤدي مراقبة الفضاء الإلكتروني الشديدة للدول إلى الحد من الحرية التي يتسم بها الإنترنت.

أن القانون الدولي القائم ينطبق على الفضاء الإلكتروني ولا حاجة لإعداد إطار قانوني جديد؛ ويجدر اعتماد مبادئ للسلوك بين الدول اعتمادا طوعيا، وإعداد تدابير من شأنها تعزيز الثقة بين الدول، هذا هو الموقف الذي تدافع عنه فرنسا وشركاؤها الأوروبيون.

وتؤدي فرنسا دورا فاعلا في عمليات التبادل الدولية بشأن الفضاء الإلكتروني، ولاسيما في إطار الأمم المتحدة، وتساهم في رسم سياسات الدفاع عن الفضاء الإلكتروني في الاتحاد الأوروبي وفي منظمة حلف شمال الأطلسي.

---

(1) موقع وزارة الشئون الداخلية الفرنسية/ المجال الرقمي والرهانات الدولية/ تشرين الثاني/ نوفمبر 2013.

2. **المنهجية**

حتى يستوفي الموضوع أهدافه ومقاصده فقد تم تقسيم العرض إلى العناصر التالية:

مقدمة

الفقرة الأولى: ماهية الإرهاب الإلكتروني وتعريفه.

الفقرة الثانية: الإرهاب الإلكتروني وأثره.

الفصل الأول: واجهات الإرهاب الإلكتروني.

الفقرة الأولى: واجهة تصميم المواقع الإليكترونية وإنشاؤها.

الفقرة الثانية: واجهة اختراق وقرصنة المواقع الإليكترونية

الفقرة الثالثة: نظام المراسلات الإليكترونية والمحادثة الآتية.

الفصل الثاني: الإجراءات الإحترازية لمواجهة الإرهاب الإلكتروني.

الفقرة الأولى: ضبط وتصفية خدمات تصفح الإنترنت.

الفقرة الثانية: التشريعات والتقنيات الإلكترونية.

الفقرة الثالثة: الوسائل التقنية للوقاية من العمليات الإرهابية الإلكترونية

الفصل الثالث: جهود فرنسا لمكافحة الإرهاب الإلكتروني

توطئة فرنسا والإرهاب: نظرة تاريخية:

الفقرة الأولى: معالم الإستراتيجية الفرنسية في مواجهة الإرهاب الإلكتروني.

الفقرة الثانية: المجلس الوطني للرقمنة: التأسيس والمهام.

تعريف المجلس الوطني للرقمنة Le Conseil National du Numérique

مهام المجلس الوطني للرقمنة

الفقرة الثالثة: المجلس في مواجهة آخر تهديدات الإرهاب الإليكتروني

الفقرة الرابعة: الفضاء الرقمي الآمن مطلب وطني وفق رؤية دولية.

عرض للنتائج مع مناقشتها ثم طرح للتوصيات

3. **النتائج**

إن التقدم المتسارع للعلوم التقنية والوسائل المعلوماتية الذي يعرفه العصر الحديث، له من الإيجابيات والمحاسن ما يستحيل حصره، إلا أن سلبياته تكاد تكون مدمرة، ما لم يكن هناك علم وحصر ومقاومة لهذه السلبيات، فمن خلال الشبكة العنكبوتية يمكن معرفة كيفية صناعة المتفجرات، وغسيل الأموال، وصناعة القنبلة النووية، وسرقة البطاقات الائتمانية، وغسل الأدمغة واستقطابها، وتعمية العقول واستدراجها، وتدجين الإرادات وتجنيدها. ولقد أظهر تقرير لمركز الأمم المتحدة للتطوير الاجتماعي والشئون الإنسانية أن الوقاية من الاعتداءات وجرائم الكمبيوتر تعتمد على المؤسسات الأمنية في إجراءات معالجة المعلومات والبيانات الإلكترونية، وتعاون ضحايا جرائم الكمبيوتر مع رجال الأمن.

فلقد أصبح الإرهاب الإلكتروني هاجسا يخيف العالم الذي أصبح عرضة لهجمات الإرهابيين عبر الإنترنت الذين يمارسون نشاطهم التخريبي من أي مكان في العالم، وهذه المخاطر تتفاقم بمرور كل يوم، لأن التقنية الحديثة وحدها غير قادرة على حماية الناس من العمليات الإرهابية الإلكترونية والتي سببت أضراراً جسمية على الأفراد والمنظمات والدول. ولقد سعت العديد من الدول من ضمنها الجمهورية الفرنسية إلى اتخاذ التدابير والاحترازات لمواجهة الإرهاب الإلكتروني، إلا أن هذه الجهود لا تزال بحاجة إلى المزيد التمحيص والمثابرة لمواجهة هذا السلاح الخطير.

فالإرهاب الإلكتروني أصبح خطراً يهدد العالم بأسره ويكمن الخطر في سهولة استخدام هذا السلاح مع شدة أثره وضرره، فيقوم مستخدمه بعمله الإرهابي وهو بعيد عن محل هذا الاعتداء.

رغم تكاثف الجهود الدولية والإقليمية ورغم النجاحات (والاخفاقات) في معالجة الظاهرة الإرهابية عربيا وأمميا فإن المقاربة الأمنية وحدها، تبقى قاصرة وعاجزة بل ونسبية أمام تعدد أبعاد الإرهاب عموما والإرهاب الإليكتروني خصوصا، ويبقي السؤال المطروح – هنا – إلى أي مدي يعتبر تبني المقاربة الزمنية (غربية الأصل والمنشأ) والاحتشاد حولها حلا لمعالجة قضايا الإرهاب وعلى رأسها الإرهاب الإليكتروني؟

إن المستقبل هو الكفيل بأن يوجه عناية الرأي العام المحلي والإقليمي والدولي إلى البحث والتنقيب عن مقاربات إبداعية وعلاجية خلافة تستنبط أساسا من مقاصد الشرع الإسلامي الحنيف واستشرافا لمستقبل إنساني آمن في ظل تعايش إنساني متعدد جوهره كنهه الرحمة للعالمين.

4. المناقشة و/ أو الاستنتاجات

إن معالجة مثل هذه الظاهرة السرطانية التي عمت بلواها العالم بأسره لا ولن تتأتي إلا بشيء وحيد: التمسك بالقرآن الكريم وتدبر معجزاته، فهما وسلوكا ومنهجا [1]، مصداقاً لأحاديث رسول الله صلي الله عليه وسلم ومنها:

1) حدثنا أبو خالد الأحمر عن عبد الحميد بن جعفر عن سعيد بن أبي سعيد عن أبي شريح الخزاعي قال: خرج علينا رسول الله صلي الله عليه وسلم فقال: أبشروا أبشروا؛ أليس تشهدوا أن لا إله إلا الله وأني رسول الله؟ قالوا: نعم، قال: فإن هذا القران سبب طرفه بيد الله وطرفه بأيديكم فتمسكوا به، فإنكم لن تضلوا ولن تهلكوا بعده أبدا [2].

2) حدثنا حسين بن علي عن حمزة الزيات عن أبي المختار الطائي عن ابن أخي الحارث الأعور عن الحارث عن علي قال: سمعت رسول الله صلي الله عليه وسلم يقول: كتاب الله فيه خبر ما قبلكم ونبأ ما بعدكم وحكم ما بينكم، هو الفصل ليس بالهزل، هو الذي لا تزيغ به الأهواء، ولا يشبع منه العلماء، ولا يخلق عن كثرة رد، ولا تنقضي عجائبه، هو الذي من تركه من جبار قصمه الله، ومن ابتغي الهدى في غيره أضله الله، هو حبل الله المتين وهو الذكر الحكيم، وهو الصراط المستقيم، هو الذي من عمل به أجر، ومن حكم به عدل، ومن دعا إليه هدي إلى صراط مستقيم، خذها إليك يا أعور [3].

3) حدثنا أبو معاوية الهجري عن أبي الأحوص عن عبد الله قال: قال رسول الله صلي الله عليه وسلم: إن هذا القران مأدبة الله فتعلموا من مأدبة الله ما استطعتم، إن هذا القرآن هو حبل الله وهو النور البين والشفاء النافع، عصمة لمن تمسك به، ونجاة لمن تبعه لا يعوج فيقوم، ولا يزيغ فيستعتب، ولا تنقضي عجائبه، ولا يخلق من كثرة الرد [4].

هذه إذا رسالة "خطيرة" واعية في طيها وصفة ربانية – نبوية كاملة، فهل من عاقل يحب أن يسعد!؟

5. التوصيات

1. الحاجة إلى موسوعة عربية وأخرى عالمية تكون مرجعا خاصا للمهتمين بالبحث في قضايا الإرهاب عموما والإرهاب الإلكتروني على وجه الخصوص.
2. تضافر جهود كافة المؤسسات العاملة في الفضاء الرقمي لإنشاء قاعدة بيانات لجرد جميع المعطيات الخاصة بالإرهاب الإليكتروني.
3. توجيه عناية السلطات الوصية على قطاع التربية والتعليم إلى وضع برامج وخطط تتضمن التوعية بقضايا الإرهاب الإليكتروني وكيفية محاربته في المؤسسات التربوية والتعليمية.
4. تحفيز منظمات المجتمع المدني للعمل على إعداد برامجها وأنشطتها وفعالياتها للتوعية الاستباقية بغاية منع وقوع جرائم الإرهاب الإلكتروني.
5. إصدار دلائل وتعميمها على أوسع نطاق قصد الإلمام بطرق استعمال التقنيات الحديثة وتفادي وقوع المستخدم ضحية للجرائم الإرهابية ذات الطابع الإلكتروني.
6. اعتماد أصول المنهاج النبوي في تجديد المقاربة العلاجية لآفة الإرهاب الإليكتروني جنبا إلى جنب مع الدراسات النظرية والتطبيقية المعاصرة بتنسيق ومشاركة علماء النصوص وعلماء الواقع لبناء رؤية ومقاربة إبداعية متجددة ورائدة ذات أصالة ومصداقية.

المراجع

(1) القران الكريم

(2) صحيح مسلم

(3) عبد الله بن محمد بن أبي شيبة/ المصنف/ دار الفكر سنة النشر: 1414هـ/ 1994م.

(4) مجمع الفقه الإسلامي/ قرارات وتوصيات الدورة الرابعة عشرة للمجلس/ قطر/ 1423هـ.

(5) د. سهير حجازي/ التهديدات الإجرامية للتجارة الإلكترونية/ شرطة دبي.

(6) موزة المزروعي/ الاختراقات الإلكترونية خطر كيف نواجهه/ مجلة آفاق الاقتصادية، دولة الإمارات العربية المتحدة، العدد التاسع، سبتمبر 2000م، ص 54.

(7) عماد علي الخليل/ التكييف القانوني الإسادة استخدام أرقام البطاقات عبر شبكة الإنترنت دراسة علمية في ظل أحكام قانون العقوبات الأردني/ بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت/ جامعة الإمارات العربية المتحدة/ ماي 2000.

(8) محمد القاسم (ضمن فريق عمل)/ دراسة الوضع الراهن في مجال أحكام في المعلوماتية/ مشروع الخطة الوطنية لتقنية المعلومات.

---

[1] وهذا أحد أوجه الإعجاز العلمي في القران الكريم التي على أهل الاختصاص الكشف عن دقائق معانيه في الآيات المتعلقة بالعلوم الكونية في ضوء أصول التفسير ووجوه الدلالة اللغوية ومقاصد الشريعة الإسلامية دون إغفال تنسيق الجهود المبذولة في العالم في مجال الإعجاز العلمي في القران والسنة والتعاون مع المؤسسات والمراكز ذات الاختصاص.

[2] عبد الله بن محمد بن أبي شيبة/ المصنف/ دار الفكر سنة النشر: 1414هـ/ 1994م.

[3] عبد الله بن محمد بن أبي شيبة/ المصنف/ دار الفكر سنة النشر: 1414هـ/ 1994م.

[4] عبد الله بن محمد بن أبي شيبة/ المصنف/ دار الفكر سنة النشر: 1414هـ/ 1994م.

(9) محمد أمين الرومي/ جرائم الكمبيوتر والإنترنت/ دار المطبوعات الجامعية، الإسكندرية/ 2003.
(10) السيد عتيق/ جرائم الإنترنت/ دار النهضة العربية، القاهرة/ 2002.
(11) صالح المسند، عبد الرحمن الجهني/ جرائم الحاسب الآلي، الخطر الحقيقي في عهد المعلومات، أكاديمية نايف للعلوم الأمنية، مجلدة 15 عدد 29 الرياض/ 2002.
(12) الدكتور أحمد فتحي سرور/ حكم القانون في مواجهة الإرهاب (القاهرة: سنة 2007) راجع مجلة جوست عدالة.
(13) موقع وزارة الشئون الخارجية الفرنسية/ المجال الرقمي والرهانات الدولية/ تشرين الثاني/ نوفمبر 2013.
(14) عبد الله عبد الكريم عبد الله/ جرائم المعلوماتية والإنترنت (الجرائم الإلكترونية)/ منشورات الحلبي الحقوقية 2007.
(15) علي أنيس/ الإنترنت وأثره على الشباب والأسرة الجهاز القومي لتنظيم الاتصالات القاهرة نوفمبر 2006.
(16) موضي بنت عبد الله آل سعود/ دور مراكز المعلومات في دعم القرار السياسي ورقة عمل مقدمة إلى مؤتمر تقنية المعلومات والأمن الوطني الرياض 2007.
(17) عبد الرحيم صدق/ الإرهاب السياسي والقانون الجنائي/ دار النهضة العربية – القاهرة، 1985م.
(18) الدكتور حسن بن محمد سفر/ الإرهاب والعنف في ميزان الشريعة الإسلامية والقانون الدولي/ بحث مقدم لمجمع الفقه الإسلامي الدولي، الدورة الرابعة عشرة، الدوحة – قطر 11 1 2003م.
(19) برهان الدين إبراهيم بن محمد بن فرحون اليعمري المالكي/ تبصرة الحكام في أصول الأقضية ومناهج الأحكام/ تخريج جمال مرعشلي/ دار الكتب العلمية، بيروت، لبنان.
(20) د. محمد بن عبد الله القاسم، د رشيد الزهراني، عبد الرحمن بن عبد الله السند، عاطف العمري/ تجارب الدول في مجال أحكام في المعلوماتية/ مشروع الخطة الوطنية لتقنية المعلومات، 1423هـ.
(21) سايمون كولن/ التجارة على الإنترنت/ نقله إلى العربية، يحيى مصلح، بيت الأفكار الدولية بأمريكا 1999م.
(22) د. عبادة أحمد عبادة/ التدمير المتعمد لأنظمة المعلومات الإلكترونية/ مركز البحوث والدراسات، شرطة دبي بدولة الإمارات العربية المتحدة.
(23) د خالد بن محمد الطويل/ التعامل مع الاعتداءات الإلكترونية من الناحية الأمنية/ مركز المعلومات الوطني، وزارة الداخلية، ورقة عمل مقدمة لورشة العمل الثالثة أحكام في المعلوماتية الذي نظمه مشروع الخطة الوطنية لتقنية المعلومات 19 10 1423هـ الرياض.
(24) عماد علي الخليل/ التكييف القانوني لإساءة استخدام أرقام البطاقات عبر شبكة الإنترنت/ بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، الذي نظمته كلية الشريعة والقانون، بجامعة الإمارات العربية المتحدة، عام 2000م.
(25) د. سهير حجازي/ التهديدات الإجرامية للتجارة الإلكترونية/ مركز البحوث والدراسات، شرطة دبي بدولة الإمارات العربية المتحدة.
(26) د. ممدوح عبد الحمد عبد المطلب/ جرائم استخدام شبكة المعلومات العالمية الجريمة عبر الإنترنت/ بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، بجامعة الإمارات العربية المتحدة، عام 2000م.
(27) قرارات وتوصيات مجمع الفقه الإسلامي، منظمة المؤتمر الإسلامي، جدة، دار القلم، دمشق.
(28) طارق بن عبد الله الشدي/ مقدمة في الحاسب الآلي وتقنيات المعلومات/ دار الوطن للنشر، الرياض، الطبعة الثانية، 1416هـ.
(29) Nothalie cettina; the French approach: Vigaur and vigilonce, (in Marianne Van levrven, confronting terrorism, ap. cit., p. 71 etc.
(30) La loi no 2006-64 du 23 janvier 2006 relative a la lutte contre le terrorism, rev. sc crim 2006, no 2, p366
(31) La France face au terrorisme : Livre blanc du Gouvernement sur la sécurité intérieure face au terrorisme [texte imprimé] / France. Premier Ministre ; France, Secrétaire . - Paris : La Documentation française, 2006. -1 vol. (141 p.) ; 24 cm. ISBN : 978- 2-11-006101-0, Langues : Français (fre)
(32) JH (2006).« La France face au terrorisme. Livre blanc du gouvernement sur la sécurité intérieure face au terrorisme. », La Documentation Française. Paris, 2006, 141 p, http://www.dsi-presse.com/?p=1494 .(Consulté le 16/09/2014)
(33) Sarkozy installe le Conseil national du numérique, Acteurs publics.com, Antoine Laurent, 27 avril 2011
(34) Le Conseil national du numérique, l'élite des professionnels de l'économie numérique, Actualités du droit, Marlène Trézéguet, 4 mai 2011
(35) Nicolas Sarkozy officialise le Conseil national du numérique, Le Nouvel Observateur, 27 mars 2011